PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 7 : G06F 1/00 — A1

(11) International Publication Number: **WO 00/45245**

(43) International Publication Date: 3 August 2000 (03.08.00)

(21) International Application Number: PCT/US99/31053

(22) International Filing Date: 28 December 1999 (28.12.99)

(30) Priority Data:
09/240,948 29 January 1999 (29.01.99) US

(71) Applicant: MOTOROLA INC. [US/US]; 1303 East Algonquin Road, Schaumburg, IL 60196 (US).

(72) Inventors: SANA, Ramna, Mona; 7040 N. 40th Street, Paradise Valley, AZ 85253 (US). FREEMAN, Nancy, Louise; 1721 N. Amber Street, Mesa, AZ 85203 (US). COVEY, Carlin, Raymond; 8637 E. Palm Lane, Scottsdale, AZ 85257 (US).

(74) Agents: INGRASSIA, Vincent, B. et al.; Motorola Inc., P.O. Box 10219, Scottsdale, AZ 85271–0219 (US).

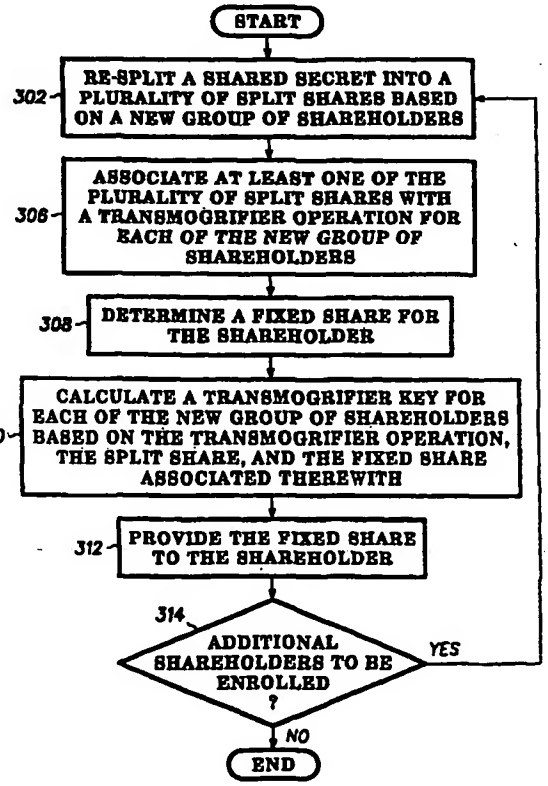
(81) Designated States: AE, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, DE, DK, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, UA, UG, UZ, VN, YU, ZA, ZW, ARIPO patent (GH, GM, KE, LS, MW, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published
With international search report.
Before the expiration of the time limit for amending the claims and to be republished in the event of the receipt of amendments.

(54) Title: METHOD FOR CONTROLLING ACCESS TO A SHARED SECRET

(57) Abstract

A method for controlling access to a shared secret includes methods (300, 400) for enrolling and disenrolling shareholders of the shared secret. The methods (300, 400) include steps which allow each shareholder to retain fixed shares associated with the shared secret while preserving the integrity of the shared secret. A method (500) for recovering the shared secret includes a step of computing (508) split shares for shareholders given a fixed share and a transmogrifier key associated with each. The fixed shares and transmogrifier keys are combined (510) for recovering the split shares which are further used when recovering the shared secret.



FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	ES	Spain	LS	Lesotho	SI	Slovenia
AM	Armenia	FI	Finland	LT	Lithuania	SK	Slovakia
AT	Austria	FR	France	LU	Luxembourg	SN	Senegal
AU	Australia	GA	Gabon	LV	Latvia	SZ	Swaziland
AZ	Azerbaijan	GB	United Kingdom	MC	Monaco	TD	Chad
BA	Bosnia and Herzegovina	GE	Georgia	MD	Republic of Moldova	TG	Togo
BB	Barbados	GH	Ghana	MG	Madagascar	TJ	Tajikistan
BE	Belgium	GN	Guinea	MK	The former Yugoslav Republic of Macedonia	TM	Turkmenistan
BF	Burkina Faso	GR	Greece			TR	Turkey
BG	Bulgaria	HU	Hungary	ML	Mali	TT	Trinidad and Tobago
BJ	Benin	IE	Ireland	MN	Mongolia	UA	Ukraine
BR	Brazil	IL	Israel	MR	Mauritania	UG	Uganda
BY	Belarus	IS	Iceland	MW	Malawi	US	United States of America
CA	Canada	IT	Italy	MX	Mexico	UZ	Uzbekistan
CF	Central African Republic	JP	Japan	NE	Niger	VN	Viet Nam
CG	Congo	KE	Kenya	NL	Netherlands	YU	Yugoslavia
CH	Switzerland	KG	Kyrgyzstan	NO	Norway	ZW	Zimbabwe
CI	Côte d'Ivoire	KP	Democratic People's Republic of Korea	NZ	New Zealand		
CM	Cameroon			PL	Poland		
CN	China	KR	Republic of Korea	PT	Portugal		
CU	Cuba	KZ	Kazakstan	RO	Romania		
CZ	Czech Republic	LC	Saint Lucia	RU	Russian Federation		
DE	Germany	LI	Liechtenstein	SD	Sudan		
DK	Denmark	LK	Sri Lanka	SE	Sweden		
EE	Estonia	LR	Liberia	SG	Singapore		

METHOD FOR CONTROLLING ACCESS TO A SHARED SECRET

Field of the Invention

This invention relates in general to a method for controlling access to a shared secret, and more specifically, to enrolling and disenrolling shareholders of the shared secret, and recovering the shared secret by combining shares associated with shareholders.

Background of the Invention

Current methods for enrolling new shareholders in a generalized secret sharing scheme (SSS) typically require new "fixed shares" to be assigned to previously enrolled shareholders. A problem with such SSS schemes is when a new shareholder is enrolled, it may be inconvenient, impractical, or impossible to provide an existing shareholder with a new fixed share. For example, when existing shareholder S_A is a member of two groups of shareholders, and each group is capable of recovering a split share of a shared secret, current methods for enrolling a new shareholder typically require that shareholder S_A receive a new fixed share. When unavailable to receive a new fixed share, shareholder S_A is effectively disenrolled from both groups of shareholders.

Likewise, methods for disenrolling a shareholder typically require that when a shareholder is removed from a group of shareholders, the remaining shareholders receive new fixed shares associated with a shared secret.

Another problem with existing methods arise when recovering a shared secret. Typical systems fail to "decouple" fixed shares associated with a shareholder when the shareholder no longer needs access to the shared secret. In other words, once a shareholder is associated with a fixed share, the shareholder has an ability to recover, at least in cooperation with other shareholders, the shared secret.

Thus, what is needed is a method for enrolling a shareholder as one of an existing group of shareholders while allowing the existing group of shareholders to retain fixed shares associated with a shared secret. What is also needed is a method for disenrolling a shareholder as one of a group of shareholders while allowing the group of shareholders, less the disenrolled shareholder, to retain fixed shares associated with a shared secret. What is also needed is a method for recovering a shared secret that decouples shareholders from the shared secret.

Brief Description of the Drawings

The invention is pointed out with particularity in the appended claims. However, a more complete understanding of the present invention may be derived by referring to the detailed description and claims when considered in connection with the figures, wherein like reference numbers refer to similar items throughout the figures and:

FIG. 1 shows a simplified block diagram of a system for controlling access to a shared secret in accordance with a preferred embodiment of the present invention;

FIG. 2 shows a simplified block diagram of a hierarchical secret sharing system for controlling access to a shared secret in accordance with a preferred embodiment of the present invention;

FIG. 3 shows a simplified flowchart of a method for enrolling a shareholder in accordance with a preferred embodiment of the present invention;

FIG. 4 shows a simplified flowchart of a method for disenrolling a shareholder in accordance with a preferred embodiment of the present invention; and

FIG. 5 shows a simplified flowchart of a method for recovering a secret in accordance with a preferred embodiment of the present invention.

The exemplification set out herein illustrates a preferred embodiment of the invention in one form thereof, and such exemplification is not intended to be construed as limiting in any manner.

Detailed Description of the Preferred Embodiment

The present invention provides, among other things, a method for enrolling and a method for disenrolling shareholders of a shared secret. The enrollment and disenrollment methods allow each shareholder to retain fixed shares associated with the shared secret when adding and removing shareholders. The integrity of the shared secret is preserved even though shareholders retain the fixed shares. The present invention also provides a method for decoupling a shareholder from a shared secret when recovering the shared secret.

A shareholder is defined herein to mean a person, a secure identification (ID) card, a FORTEZZA card, a smart card, a credit card, a debit card, a cellular telephone, a satellite phone, a pager, a radio, a satellite, a security device, a computer, a peripheral device, a personal digital assistant, etc., capable of storing and recalling a fixed share, such as, for example, a security token, a password, a pin number, a cryptographic key, a digital signature, a share of a shared secret, a shared secret, etc. A group of shareholders is defined herein to mean a collection of individual shareholders as described above. Preferably, groups of shareholders are comprised of a combination of similar types of shareholders, however the present invention may include a combination of different types of shareholders (e.g., a satellite phone and a satellite).

A shared secret is defined herein to mean a piece of information that may be split into pieces of information (e.g., shares) to be distributed to shareholders. In accordance with a preferred embodiment of the present invention, no share reveals the shared secret or any part of any other share with regard to the shared secret. A secret sharing scheme splits a shared secret into shares, and recombines split shares to recover the shared secret. A threshold secret sharing scheme combines at least some minimum number of fixed shares to recover a shared secret. In accordance with the preferred embodiment of the present invention, a threshold scheme is an M-of-N scheme, wherein M and N are positive integers and M is less than or equal to N. Preferably, M represents the minimum number of shares needed to recover the secret, and N represents the total number of shares that are distributed. A generalized secret sharing (GSS) scheme combines a number of fixed shares to recover a split share, and combines a number of split shares to recover a shared secret. In accordance with the preferred embodiment of the present invention, in a GSS scheme, two or more groups of shareholders shares can be combined to recover a shared secret.

A split share is defined herein to mean a share that when combined with a predetermined number of other split shares recovers a shared secret. A fixed share is

defined herein to mean a share stored by and recoverable from a shareholder. In accordance with the preferred embodiment of the present invention, when a fixed share is combined with an associated transmogrifier key via a transmogrifier operation, a split share is recovered. A transmogrifier key is defined herein to mean a value which is stored by and recoverable from a system element (e.g., a computer, a programmable logic device, a smart card, etc.). Preferably, the system element also associates the transmogrifier key with a split share.

A transmogrifier operation is defined herein to mean an operation that is a function in a forward direction and a relation in a reverse direction. In other words, when a forward transmogrifier operation receives two inputs (e.g., a fixed share and a transmogrifier key), a single output is generated (e.g., a split share). However, when a reverse transmogrifier operation receives two inputs (e.g., a split share and a fixed share) one or more outputs are generated (e.g., transmogrifier key). Preferably, any one of the transmogrifier keys may be associated with the fixed share. Examples of transmogrifier operations include, for example, addition, subtraction, exclusive-or, quadratic equations, cubic equations, elliptic-curve equations, etc.

FIG. 1 shows a simplified block diagram of a system for controlling access to a shared secret in accordance with a preferred embodiment of the present invention. In a preferred embodiment of the present invention, system 100 includes transmogrifiers 108-110 and share combiner 114. In one preferred embodiment, transmogrifiers 108-110 and share combiner 114 are implemented as, for example, software programs executing on a computer. In another preferred embodiment, transmogrifiers 108-110 and share combiner 114 are implemented in hardware such as, for example, a programmable logic device. In other embodiments, combinations of software and hardware may be used to implement transmogrifiers 108-110 and share combiner 114.

In a preferred embodiment, transmogrifiers 108-110 receive fixed shares 102-104. Transmogrifiers 108-110 perform a transmogrifier operation on inputs of fixed shares 102-104 and transmogrifier keys 105-107, and generate split shares 111-113. Share combiner 114 preferably combines split shares 111-113 to generate shared secret 116. In a preferred embodiment, share combiner 114 combines split shares by performing a secret sharing scheme.

In a preferred embodiment, each transmogrifier operation performed by transmogrifiers 108-110 comprises substantially the same (e.g., homogenous) operation such as, for example, addition on its respective inputs. In another embodiment, each transmogrifier operation performed by transmogrifiers 108-110 comprises a unique (e.g., heterogeneous) operation, such as, for example, addition,

subtraction, and exclusive-or. In other words, each of the transmogrifiers shown in system 100 performs a unique operation on the respective inputs. For example transmogrifier 108 performs an addition operation, transmogrifier 109 performs a subtraction operation, and transmogrifier 110 performs an exclusive-or operation.

FIG. 2 shows a simplified block diagram of a hierarchical secret sharing system for controlling access to a shared secret in accordance with a preferred embodiment of the present invention. In a preferred embodiment of the present invention, system 200 generally includes a plurality of system 100 (FIG. 1) elements and a share combiner 114. In a preferred embodiment, system 200 includes combinations of system 100 elements arranged such that outputs of system 100 elements generate shared secrets 116. Preferably, shared secrets 116 are input to share combiner 114 to recover a "high level" shared secret. In another embodiment, combinations of system 200 elements are arranged such that an output of share combiner 114 is input to other system 200 elements.

Similar to that for elements in system 100 (FIG. 1), system 200 elements are preferably implemented as software programs. In another embodiment, system 200 elements may be implemented as hardware devices such as, for example, programmable logic devices. In another embodiment, system 200 elements may be implemented as a combination of hardware and software elements.

FIG. 3 shows a simplified flowchart of a method for enrolling a shareholder in accordance with a preferred embodiment of the present invention. In a preferred embodiment, method 300 is performed for enrolling a shareholder as one of a group of shareholders of a shared secret. In a preferred embodiment, method 300 is performed for enrolling a shareholder in a system implementing a generalized secret sharing scheme for a shared secret. In another embodiment, method 300 is performed for enrolling a shareholder in a system implementing a threshold sharing scheme for a shared secret. In a preferred embodiment, method 300 is performed by a system, for example system 200 (FIG. 2), implementing a generalized secret sharing scheme. In another embodiment, method 300 is performed by a system, for example system 100, implementing a threshold sharing scheme.

In a preferred embodiment, method 300 is performed for enrolling a shareholder as one of a group of shareholders to create a new group of shareholders. Each of the group of shareholders retains fixed shares associated with a shared secret determined prior to enrolling the shareholder. Preferably, method 300 is implemented as a set of steps, for example, steps 302-314.

In step 302, the shared secret is re-split into a plurality of split shares. In a preferred embodiment, a method such as, for example, Shamir's secret sharing

scheme is performed to split the shared secret. Preferably, the number splits is equivalent to the number of shareholders in the new group of shareholders. In other embodiments, methods such as, for example, Blakley's geometric scheme", "Benaloh-Leichter scheme", "Generalized Secret Sharing and Monotone Functions", "Brickell-Davenport scheme", and "Ito-Saito-Nishizeki scheme" are also suitable for splitting the shared secret.

In step 306, at least one of the plurality of split shares is associated with a transmogrifier operation for each of the new group of shareholders. In a preferred embodiment, a transmogrifier operation is associated with a split share. Preferably, each split share is associated with one transmogrifier operation.

In step 308, a fixed share is determined for the shareholder. In a preferred embodiment, a fixed share is generated by a random number generator. In other embodiments, other methods of determining a fixed share include, for example, selecting a fixed share from a large pool of fixed shares. In yet another embodiment, a shareholder may retain a fixed share determined prior to performing step 308.

In step 310, a transmogrifier key is calculated for each of the new group of shareholders. In a preferred embodiment, a transmogrifier key is computed by determining a value that when combined with a fixed share and operated on by an associated transmogrifier operation, generates a split share for each shareholder.

In step 312, the fixed share is provided to the shareholder. In a preferred embodiment, the shareholder receives the fixed share determined in step 308. As discussed in step 308, a shareholder may retain a fixed share that was previously determined.

In step 314, a check is performed to determine when additional shareholders are to be enrolled. In a preferred embodiment, when no additional shareholders are to be enrolled, the method ends. Otherwise, step 302 is performed.

FIG. 4 shows a simplified flowchart of a method for disenrolling a shareholder in accordance with a preferred embodiment of the present invention. In a preferred embodiment, method 400 is for disenrolling a shareholder as one of a group of shareholders of a shared secret. In a preferred embodiment, method 400 is for disenrolling a shareholder in a system implementing a generalized secret sharing scheme for a shared secret. In another embodiment, method 400 is for disenrolling a shareholder in a system implementing a threshold sharing scheme for a shared secret. In a preferred embodiment, method 400 is performed by a system, for example system 200 (FIG. 2), implementing a generalized secret sharing scheme. In another embodiment, method 400 is performed by a system, for example system 100, implementing a threshold sharing scheme.

In a preferred embodiment, method 400 is for disenrolling a shareholder as one of a group of shareholders to create a new group of shareholders. Each of the new group of shareholders retains fixed shares associated with a shared secret determined prior to disenrolling the shareholder. Preferably, method 400 is implemented as a set of steps, for example, steps 406-412.

In step 406, the shared secret is re-split into a plurality of split shares based on the new group of shareholders. In a preferred embodiment, a method such as, for example, Shamir's secret sharing scheme is performed to split the shared secret. Preferably, the number of splits is equivalent to the number of shareholders in the new group of shareholders.

In step 408, at least one of the plurality of shares is associated with a transmogrifier operation for each of the new group of shareholders. In a preferred embodiment, each split share is associated with one transmogrifier operation.

In step 410, a transmogrifier key is calculated for each of the new group of shareholders. In a preferred embodiment, a transmogrifier key is computed by determining a value that when combined with a fixed share and operated on by an associated transmogrifier operation, generates a split share for each shareholder.

In step 412, a check is performed to determine when another shareholder is to be disenrolled. In a preferred embodiment, when another shareholder is to be disenrolled, step 402 is performed. Otherwise, the method ends.

FIG. 5 shows a simplified flowchart of a method for recovering a secret in accordance with a preferred embodiment of the present invention. In a preferred embodiment, method 500 is performed to recover a shared secret for a system implementing a generalized secret sharing scheme. In another embodiment, method 500 is performed to recover a shared secret for a system implementing a threshold sharing scheme.

In a preferred embodiment, method 500 generally includes a set of steps for recovering a shared secret. Preferably, shareholders of a shared secret provide fixed shares to a transmogrifier operation. The transmogrifier operation combines the fixed shares with an associated transmogrifier key to recover a split share. A share combiner preferably combines the split shares to recover the shared secret. In a preferred embodiment, method 500 is implemented as a set of steps, for example, steps 502-516.

In step 502, a fixed share is received from each of a group of shareholders. In a preferred embodiment, a transmogrifier receives a fixed share from each of the group of shareholders. In another embodiment, a number of shareholders less than all the group of shareholders is needed to recover the shared secret. Therefore, in the

other embodiment, the number of fixed shares received in step 502 is less than the number of shareholders in the group.

In step 504, a transmogrifier key is associated with each of the group of shareholders. In a preferred embodiment, a transmogrifier key is associated with each fixed share received in step 502 for each of the group of shareholders. Preferably, a one-to-one relationship exists between fixed shares and transmogrifier keys.

In step 508, a split share is computed for each of the group of shareholders. In a preferred embodiment, a transmogrifier operation associated with each shareholder is performed on the fixed share and the transmogrifier keys determined in step 504. Preferably, performing the transmogrifier operation generates a split share for each of the shareholders.

In step 510, the split shares are combined to recover the shared secret. In a preferred embodiment, the split shares determined in step 508 are combined to recover the shared secret. Preferably, a method such as Shamir's secret sharing scheme is performed to combine the split shares. In other embodiments, methods such as, for example, Blakley's geometric scheme", "Benaloh-Leichter scheme", "Generalized Secret Sharing and Monotone Functions", "Brickell-Davenport scheme", and "Ito-Saito-Nishizeki scheme" are also suitable for combining split shares to recover a shared secret.

In step 512, a check is performed to determine when another group of shareholders needs to recover a shared secret to further determine access to a high level shared secret. In a preferred embodiment, when additional shared secrets need to be recovered for further recovering a high level shared secret, step 502 is performed. Otherwise, step 514 is performed.

In step 514, a check is performed to determine when more than one group of shareholders needs to recover a shared secret. In a preferred embodiment, when more than one group of shareholders needs to recover a shared secret, for further recovering a high level shared secret, step 516 is performed. Otherwise, the method ends.

In step 516, the shared secrets are combined to recover the high level shared secret. In a preferred embodiment, a step similar to step 510 is performed to combine shared secrets to recover the high level shared secret.

Among other things, a method for enrolling and a method for disenrolling shareholders of a shared secret have been described. The enrollment and disenrollment methods allow each shareholder to retain fixed shares associated with the shared secret when adding and removing shareholders, respectively. The

integrity of the shared secret is preserved even though shareholders retain the fixed shares. What has also been shown is a method for decoupling a shareholder from a shared secret when recovering the shared secret.

Thus, a method for controlling access to a shared secret has been described which overcomes specific problems and accomplishes certain advantages relative to prior art methods and mechanisms. The improvements over known technology are significant. The inconvenience, impracticality, or impossibility of assigning new fixed shares to shareholders when adding and removing shareholders is avoided. Similarly, a shareholder, whether currently one of a group of shareholders or not, may retain a fixed share of a shared secret without compromising the integrity of the shared secret.

The foregoing description of the specific embodiments will so fully reveal the general nature of the invention that others can, by applying current knowledge, readily modify and/or adapt for various applications such specific embodiments without departing from the generic concept, and therefore such adaptations and modifications should and are intended to be comprehended within the meaning and range of equivalents of the disclosed embodiments.

It is to be understood that the phraseology or terminology employed herein is for the purpose of description and not of limitation. Accordingly, the invention is intended to embrace all such alternatives, modifications, equivalents and variations as fall within the spirit and broad scope of the appended claims.

CLAIMS

What is claimed is:

1. A method for enrolling a shareholder as a member of a group of shareholders to create a new group of shareholders, each of the group of shareholders retaining fixed shares associated with a shared secret determined prior to enrolling the shareholder, the shared secret being split into a plurality of split shares based on the new group of shareholders, the method comprising the steps of:

associating at least one of the plurality of split shares with a transmogrifier operation for the shareholder;

determining a fixed share for the shareholder;

calculating a transmogrifier key for the shareholder based on the transmogrifier operation, the at least one split share, and the fixed share; and

providing the fixed share to the shareholder.

2. The method as claimed in claim 1, wherein the calculating step further includes the step of determining the transmogrifier key by computing a value that when combined with the fixed share and operated on by the transmogrifier operation, generates the at least one split share.

3. The method as claimed in claim 1, wherein the determining step includes the step of generating a random number to compute the fixed share.

4. The method as claimed in claim 1, further comprising the steps of:

associating at least one of the plurality of split shares for each of the group of shareholders with of a set of transmogrifier operations; and

calculating a transmogrifier key for each of the group of shareholders based on the at least one of the set of transmogrifier operations, the plurality of split shares, and the fixed shares.

5. The method as claimed in claim 4, further comprising the steps of:

performing the transmogrifier operation on the fixed shares and associated transmogrifier keys of each of the new group of shareholders to recover the plurality of split share associated with each of the new group of shareholders; and

combining the plurality of split shares to recover the shared secret.

6. The method as claimed in claim 4, wherein the set of transmogrifier operations comprises a set of homogeneous operations.

7. The method as claimed in claim 4, wherein the set of transmogrifier operations comprises a set of heterogeneous operations.

8. The method as claimed in claim 4, wherein the set of transmogrifier operations comprises a first set of homogeneous operations and a second set of heterogeneous operations.

9. A method for disenrolling a shareholder as a member of a group of shareholders to create a new group of shareholders, each of the new group of shareholders retaining fixed shares associated with a shared secret determined prior to disenrolling the shareholder, the method comprising the steps of:

re-splitting the shared secret into a plurality of split shares based on the new group of shareholders;

associating at least one split share of the plurality of split shares with a transmogrifier operation for each of the new group of shareholders; and

calculating a transmogrifier key for each of the new group of shareholders based on the transmogrifier operation, the at least one split share, and at least one of the fixed shares associated therewith.

10. The method as claimed in claim 9, wherein in the calculating step further includes the step of determining the transmogrifier key by computing a value that when combined with the at least one of the fixed shares and operated on by the transmogrifier operation, generates the at least one split share.

11. The method as claimed in claim 9, wherein the transmogrifier operation for each of the new group of shareholders comprises a set of homogeneous operations.

12. The method as claimed in claim 9, wherein the transmogrifier operation for each of the new group of shareholders comprises a set of heterogeneous operations.

13. The method as claimed in claim 9, wherein the transmogrifier operation for each of the new group of shareholders comprises a first set of homogeneous operations and a second set of heterogeneous operations.

14. A method for recovering a shared secret, the method comprising the steps of:

receiving a fixed share from each of a group of shareholders;

associating a transmogrifier key with each of the group of shareholders;

computing a split share for each of the group of shareholders based on a transmogrifier operation, the transmogrifier key, and the fixed share associated therewith; and

combining the split share for each of the group of shareholders to recover the shared secret.

15. The method as claimed in claim 14, wherein the combining step comprises a threshold secret sharing scheme.

16. The method as claimed in claim 14, wherein the combining step comprises a generalized secret sharing scheme.

17. The method as claimed in claim 14, further comprising the steps of:

checking to determine when another group of shareholders needs to recover another shared secret to further recover a high level secret; and

combining the shared secret and the another shared secret to recover the high level secret.

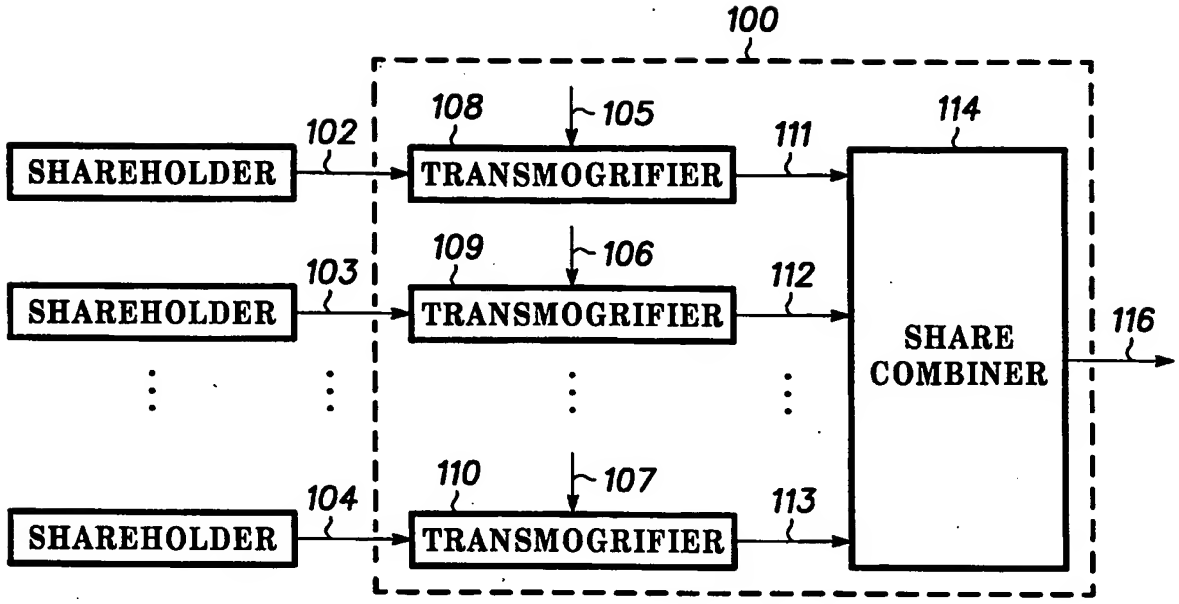

100
SHAREHOLDER
SHAREHOLDER
SHAREHOLDER
102
103
104
108
109
110
105
106
107
TRANSMOGRIFIER
TRANSMOGRIFIER
TRANSMOGRIFIER
111
112
113
114
SHARE COMBINER
116

FIG. 1

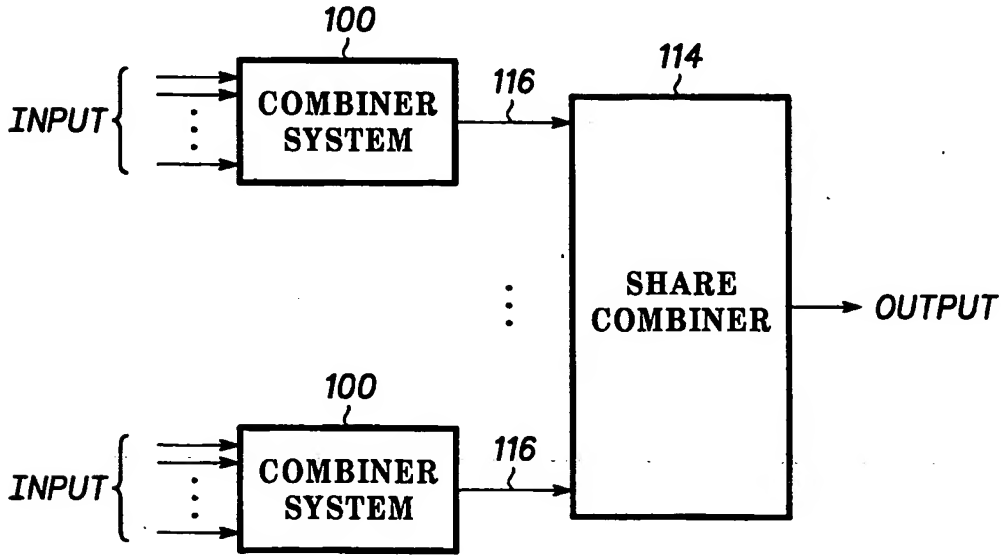

100
INPUT
COMBINER SYSTEM
116
114
SHARE COMBINER
OUTPUT
100
INPUT
COMBINER SYSTEM
116

FIG. 2

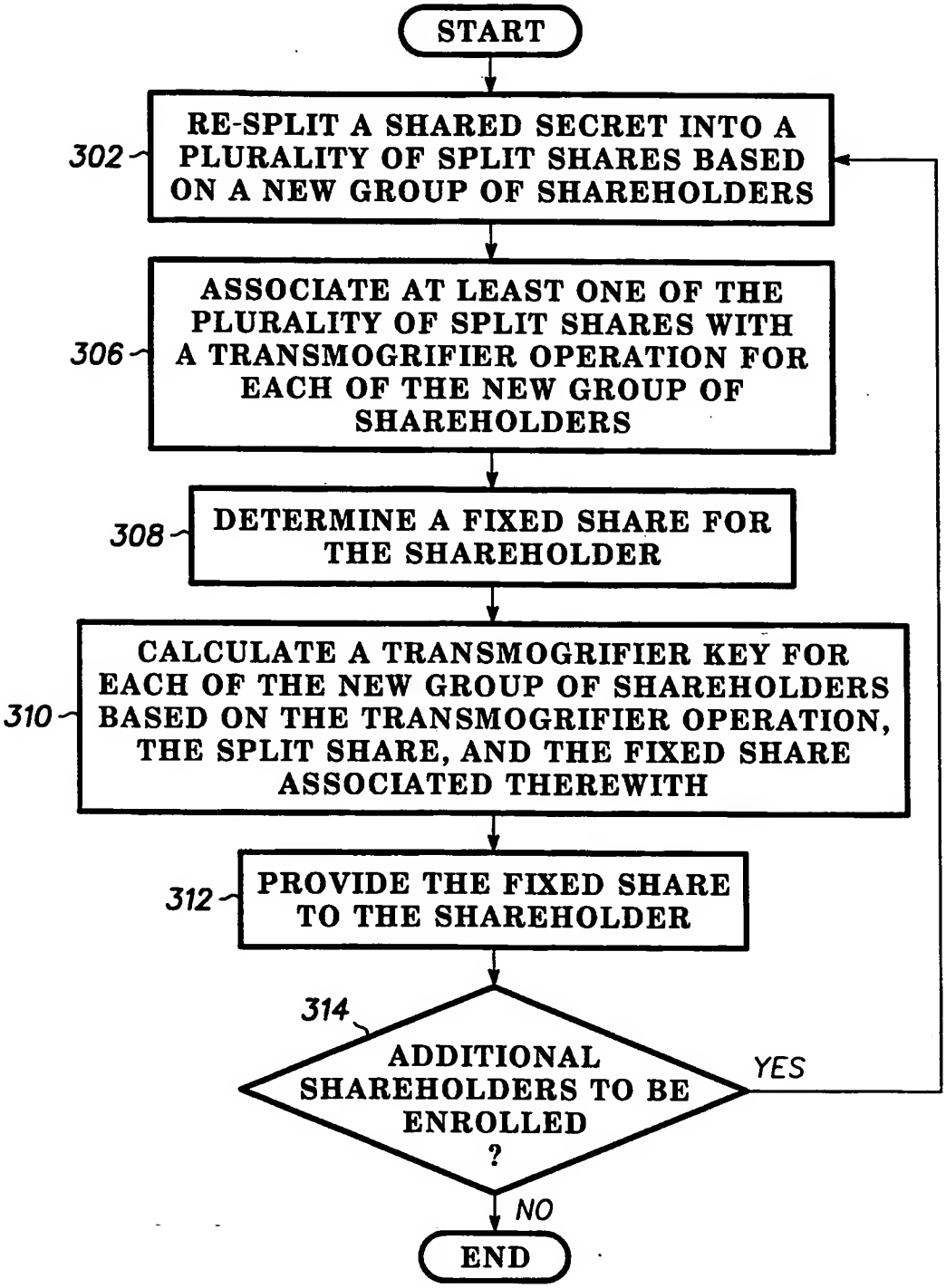

START
302
RE-SPLIT A SHARED SECRET INTO A PLURALITY OF SPLIT SHARES BASED ON A NEW GROUP OF SHAREHOLDERS
306
ASSOCIATE AT LEAST ONE OF THE PLURALITY OF SPLIT SHARES WITH A TRANSMOGRIFIER OPERATION FOR EACH OF THE NEW GROUP OF SHAREHOLDERS
308
DETERMINE A FIXED SHARE FOR THE SHAREHOLDER
310
CALCULATE A TRANSMOGRIFIER KEY FOR EACH OF THE NEW GROUP OF SHAREHOLDERS BASED ON THE TRANSMOGRIFIER OPERATION, THE SPLIT SHARE, AND THE FIXED SHARE ASSOCIATED THEREWITH
312
PROVIDE THE FIXED SHARE TO THE SHAREHOLDER
314
ADDITIONAL SHAREHOLDERS TO BE ENROLLED ?
YES
NO
END

FIG. 3

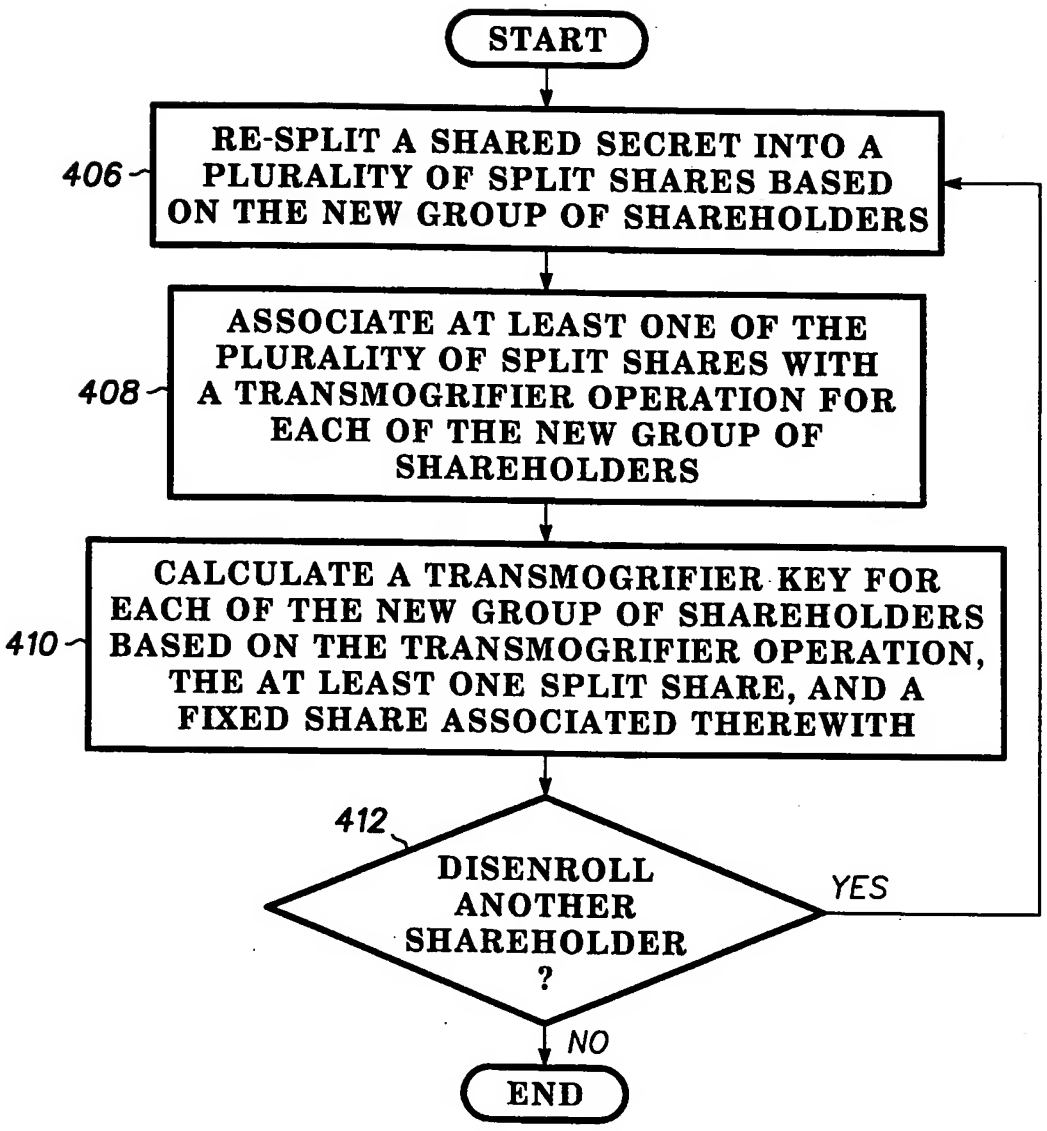

START
406
RE-SPLIT A SHARED SECRET INTO A PLURALITY OF SPLIT SHARES BASED ON THE NEW GROUP OF SHAREHOLDERS
408
ASSOCIATE AT LEAST ONE OF THE PLURALITY OF SPLIT SHARES WITH A TRANSMOGRIFIER OPERATION FOR EACH OF THE NEW GROUP OF SHAREHOLDERS
410
CALCULATE A TRANSMOGRIFIER KEY FOR EACH OF THE NEW GROUP OF SHAREHOLDERS BASED ON THE TRANSMOGRIFIER OPERATION, THE AT LEAST ONE SPLIT SHARE, AND A FIXED SHARE ASSOCIATED THEREWITH
412
DISENROLL ANOTHER SHAREHOLDER ?
YES
NO
END

FIG. 4

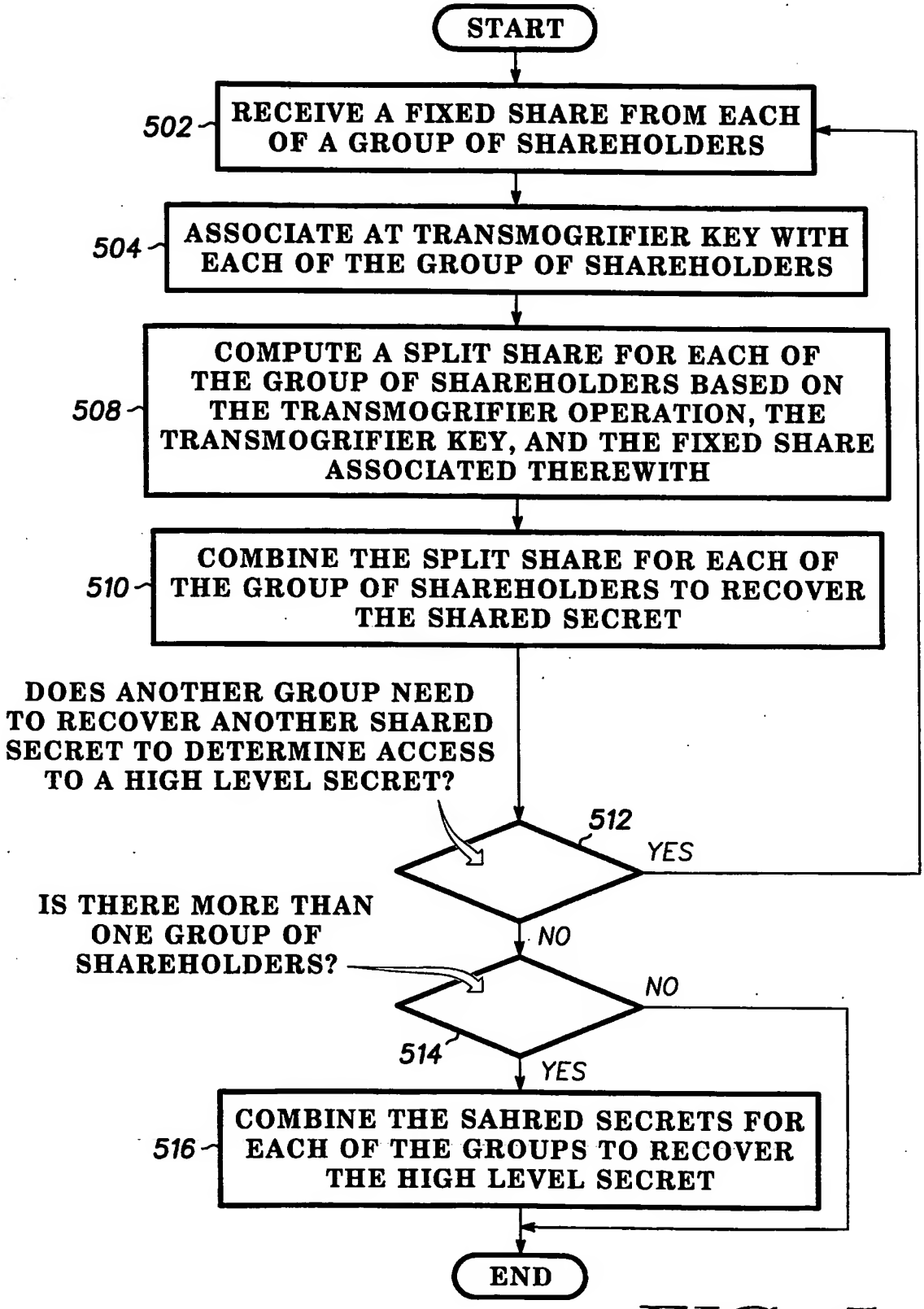

START
502
RECEIVE A FIXED SHARE FROM EACH OF A GROUP OF SHAREHOLDERS
504
ASSOCIATE AT TRANSMOGRIFIER KEY WITH EACH OF THE GROUP OF SHAREHOLDERS
508
COMPUTE A SPLIT SHARE FOR EACH OF THE GROUP OF SHAREHOLDERS BASED ON THE TRANSMOGRIFIER OPERATION, THE TRANSMOGRIFIER KEY, AND THE FIXED SHARE ASSOCIATED THEREWITH
510
COMBINE THE SPLIT SHARE FOR EACH OF THE GROUP OF SHAREHOLDERS TO RECOVER THE SHARED SECRET
DOES ANOTHER GROUP NEED TO RECOVER ANOTHER SHARED SECRET TO DETERMINE ACCESS TO A HIGH LEVEL SECRET?
512
YES
NO
IS THERE MORE THAN ONE GROUP OF SHAREHOLDERS?
NO
514
YES
516
COMBINE THE SAHRED SECRETS FOR EACH OF THE GROUPS TO RECOVER THE HIGH LEVEL SECRET
END

FIG. 5

INTERNATIONAL SEARCH REPORT

Interna al Application No
PCT/US 99/31053

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 G06F1/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	CHARNES ET AL: "Conditionally Secure Secret Sharing Schemes with Disenrollment Capability" PROCEEDINGS OF THE 2ND ACM CONFERENCE ON COMPUTER AND COMMUNICATIONS SECURITY, 2 - 4 November 1994, pages 89-95, XP002137680 Fairfax, VA, US sections 6 and 8 ---	1-17
A	CACHIN: "On-line Secret Sharing" PROCEEDINGS OF FIFTH IMA CONFERENCE ON CRYPTOGRAPHY AND CODING, 18 - 20 December 1995, pages 190-198, XP002137681 Cirencester, UK the whole document --- -/—	1-17

[X] Further documents are listed in the continuation of box C.

[ ] Patent family members are listed in annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
15 May 2000	29/05/2000

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Abram, R

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Interna ul Application No
PCT/US 99/31053

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication,where appropriate, of the relevant passages	Relevant to claim No.
A	CHEN ET AL: "Secret Sharing with Reusable Polynomials" PROCEEDINGS, INFORMATION SECURITY AND PRIVACY - SECOND AUSTRALASIAN CONFERENCE - ACISP'97, 7 - 9 July 1997, pages 183-193, XP002137682 Sydney, NSW, AU the whole document	1-17
A	LAIH ET AL: "DYNAMIC THRESHOLD SCHEME BASED ON THE DEFINITION OF CROSS-PRODUCT IN AN N-DIMENSIONAL LINEAR SPACE" PROCEEDINGS OF THE CONFERENCE ON THEORY AND APPLICATIONS OF CRYPTOLOGY,US,NEW YORK, SPRINGER, vol. CONF. 9, 1989, pages 286-298, XP002018655 the whole document	1-17

Form PCT/ISA/210 (continuation of second sheet) (July 1992)